

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA**

IN RE: DOLLAR ENERGY FUND, INC. DATA SECURITY INCIDENT LITIGATION.	Case No. 2:23-cv-01916-WSS CONSOLIDATED CLASS ACTION COMPLAINT JURY TRIAL DEMANDED
---	--

Plaintiffs Jessica Flagella, on behalf of herself and her minor children A.F. and A.F., and Cindy Tignor (“Plaintiffs”) bring this Class Action Complaint (“Complaint”) against Dollar Energy Fund, Inc. (“Dollar Energy” or “Defendant”), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels’ investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this Complaint against Dollar Energy for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including, but not limited to: full names and Social Security numbers (collectively, “personally identifiable information” or “PII”).
2. Defendant is an energy corporation that provides “utility assistance grants to families and individuals[.]”¹

¹ <https://www.dollarenergy.org/> (last accessed Oct. 30, 2023).

3. As a condition of obtaining energy products and/or services at Dollar Energy, Defendant requires that its customers, including Plaintiffs and Class Members, provide it with sensitive, non-public PII. Without the sensitive, non-public PII it collects from its customers, Defendant could not perform its regular business activities.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On February 5, 2023, Defendant “experienced a network disruption that impacted [Defendant’s] ability to access certain files on [Defendant’s] network[]” (the “Data Breach”).² Upon discovering the suspicious activity, Defendant “immediately reported the incident to law enforcement and began working with computer specialists[]” to determine the nature and scope of the Data Breach.³ As a result of that investigation, Dollar Energy concluded, on an undisclosed date, that “certain information stored on [Defendant’s] network was accessed between January 31, 2023 and February 5, 2023.”⁴

6. Defendant’s investigation concluded that the PII compromised in the Data Breach included Plaintiffs’ and approximately 28,000 other individuals’ information.⁵

² The “Notice Letter”. Sample copy available at <https://apps.web.maine.gov/online/aevviewer/ME/40/862d1222-4fd2-482b-9651-c3eea92cc6c0.shtml> (last accessed Oct. 30, 2023).

³ *Id.*

⁴ *Id.*

⁵ <https://apps.web.maine.gov/online/aevviewer/ME/40/862d1222-4fd2-482b-9651-c3eea92cc6c0.shtml> (last accessed Oct. 30, 2023).

7. According to the untitled letter that Defendant sent to Plaintiffs and Class Members (the “Notice Letter”), the compromised PII included individuals’ full names and Social Security numbers.⁶

8. Defendant failed to adequately protect Plaintiffs’ and Class Members PII—and failed to even encrypt or redact this highly sensitive information. Had this information been properly encrypted, the cybercriminals would have made off with only unintelligible data. This unencrypted, unredacted PII was compromised due to Defendant’s negligent and/or careless acts and omissions and its utter failure to protect customers’ sensitive data. Hackers targeted and obtained Plaintiffs’ and Class Members’ PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. This present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. Moreover, Defendant failed to provide Plaintiffs and Class Members with timely and adequate notice. The Data Breach occurred from January 31, 2023 through February 5, 2023,⁷ yet Defendant did not notify impacted individuals until September 28, 2023—*more than six months* following the Data Breach. During this time, Plaintiffs and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

10. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant’s failure to: (i) adequately protect the PII of Plaintiffs and Class Members; and (ii) effectively secure hardware containing protected PII using reasonable and effective

⁶ *Id.*

⁷ *Id.*

security procedures free of vulnerabilities and incidents. Defendant's conduct amounts, at least, to negligence and violates federal and state statutes.

11. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

12. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Tignor experiencing fraud in the form of an identity thief using her PII to submit a credit card application to Capital One in or about March 2023; (ix) Plaintiff Tignor experiencing fraud in the form of an identity thief using her PII to submit a credit card application to CBNA Bank in or about October 2023 and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

13. Plaintiffs and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiffs, is a citizen of a state different from Defendant.

15. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

16. Venue is proper under 18 U.S.C. § 1331(b)(1) because Defendant's principal place of business is in this District.

PARTIES

17. Plaintiff Jessica Flagella, on behalf of her minor Children AF and AF, is, and at all times mentioned herein was, an individual citizen of the State of Pennsylvania.

18. Plaintiff Cindy Tignor is, and at all times mentioned herein was, an individual citizen of the State of West Virginia.

19. Defendant Dollar Energy is an energy corporation incorporated under the state laws of Pennsylvania, with its principal office located at 15 Terminal Way, Pittsburgh, Pennsylvania 15219.

FACTUAL ALLEGATIONS

A. Defendant's Business

20. Defendant is an energy corporation that provides “utility assistance grants to families and individuals[.]”⁸

21. Plaintiffs and Class Members are current and former customers at Dollar Energy.

22. As a condition of obtaining energy products and/or services at Dollar Energy, Defendant requires its customers, including Plaintiffs and Class Members, to provide Dollar Energy with sensitive, non-public PII, which Defendant could not perform its regular business activities without.

23. The information held by Defendant in its computer systems included the unencrypted PII of Plaintiffs and Class Members.

24. Defendant recognizes the need to protect the PII that it maintains. The Privacy Policy posted on Defendant’s website provides that: “Dollar Energy Fund Inc. is committed to maintaining your confidence and trust. Therefore, the following privacy policy is in place to protect personal information you may provide online or offline.”⁹

25. Plaintiffs and Class Members entrusted their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

⁸ <https://www.dollarenergy.org/> (last accessed Oct. 30, 2023).

⁹ <https://www.dollarenergy.org/privacy-policy/> (last accessed Oct. 30, 2023).

26. Plaintiffs and the Class Members value, and have taken reasonable steps to maintain, the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

27. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

28. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

29. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

30. Plaintiffs and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of their PII.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

B. The Data Breach

32. On or about September 28, 2023, Defendant began sending Plaintiffs and other victims of an untitled Notice Letter, informing them that:

What Happened: On February 5, 2023, we experienced a network disruption that impacted our ability to access certain files on our network. We immediately reported the incident to law enforcement and began working with computer specialists. Our investigation determined that certain information stored on our network was accessed between January 31, 2023 and February 5, 2023. Therefore, in an abundance of caution, we are notifying potentially impacted individuals.

What Information Was Involved: The type of information potentially impacted may have included your name and the following: Social Security number.¹⁰

33. Omitted from the Notice Letter were the dates of Defendant's investigation, the date that Defendant detected the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, why Dollar Energy failed to notify impacted individuals about their compromised data for *more than six months* after the Data Breach's occurrence, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

34. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

35. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members,

¹⁰ Notice Letter.

causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

36. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted PII of Plaintiffs and Class Members, including their Social Security numbers and other sensitive information. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

37. Plaintiffs further believes that her PII, and that of Class Members, was subsequently offered for sale on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and the reason for executing the targeted Data Breach in the first place.

38. Plaintiffs' and Class Members' PII also could also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

C. Data Breaches Are Preventable

39. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”¹¹

40. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

¹¹ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Aug. 23, 2021).

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹²

¹² *Id.* at 3-4.

41. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹³

¹³ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 11, 2021).

42. Given that Defendant was storing the sensitive PII of its current and former customers, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

43. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of thousands of customers, including that of Plaintiffs and Class Members.

D. Defendant Acquires, Collects, And Stores Customers' PII

44. As a condition to obtain energy products and/or services from Dollar Energy, Plaintiffs and Class Members were required to give their sensitive and confidential PII to Defendant.

45. Defendant retains and stores this information and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiffs' and Class Members' PII, Defendant would be unable to provide its energy services.

46. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

47. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

48. Defendant could have prevented this targeted Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members.

49. Upon information and belief, Defendant made promises in its Privacy Policy to maintain and protect the PII collected by Defendant, demonstrating an understanding of the importance of securing PII.

50. Indeed, Defendant's Privacy Policy provides that: "Dollar Energy Fund Inc. is committed to maintaining your confidence and trust. Therefore, the following privacy policy is in place to protect personal information you may provide online or offline."¹⁴

E. Defendant Knew Or Should Have Known Of The Risk Because Energy Companies In Possession Of PII Are Particularly Susceptible To Cyber Attacks

51. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII to commit fraud or identity theft or selling it to those who would.

52. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and other sensitive information, like Defendant, preceding the date of the breach.

53. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.¹⁵

54. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion

¹⁴ <https://www.dollarenergy.org/privacy-policy/> (last accessed Oct. 30, 2023).

¹⁵ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/> (last accessed Oct. 11, 2023).

records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

55. Additionally, as companies became more dependent on computer systems to run their business,¹⁶ e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹⁷

56. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹⁸

57. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

58. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

¹⁶ <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

¹⁷ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

¹⁸ https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

59. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

60. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to tens of thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

61. In the Notice Letter, Defendant makes an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

62. Defendant's offering of credit and identity monitoring establishes that Plaintiffs' and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems and that there is a present and continued risk of misuse of that data.

63. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

64. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

65. As an energy company in custody of its current and former customers' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

F. Value Of Personally Identifiable Information

66. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁹ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."²⁰

67. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity

¹⁹ 17 C.F.R. § 248.201 (2013).

²⁰ *Id.*

credentials.²¹ For example, Personal Information can be sold at a price ranging from \$40 to \$200.²²

Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²³

68. For example, Social Security numbers, which were compromised for Plaintiffs and some Class Members as alleged herein, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.²⁴

69. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

²¹ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Oct. 17, 2022).

²² *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Oct. 17, 2022).

²³ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Oct. 217, 2022).

²⁴ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Oct. 17, 2022).

70. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”²⁵

71. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—Social Security number and name.

72. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²⁶

73. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

74. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

²⁵ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Oct. 17, 2022).

²⁶ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Oct. 17, 2022).

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁷

75. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

G. Defendant Fails To Comply With FTC Guidelines

76. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

77. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.²⁸

78. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone

²⁷ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Oct. 17, 2022).

²⁸ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).

is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²⁹

79. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

80. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

81. These FTC enforcement actions include actions against energy companies, like Defendant.

82. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant’s duty in this regard.

83. Defendant failed to properly implement basic data security practices.

²⁹ *Id.*

84. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to its customers' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

85. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

H. Defendant Fails To Comply With Industry Standards

86. As noted above, experts studying cyber security routinely identify entities in possession of PII, like Dollar Energy, as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

87. Several best practices have been identified that a minimum should be implemented by energy companies in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

88. Other best cybersecurity practices that are standard in the energy industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection

against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including by failing to train staff.

89. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

90. These foregoing frameworks are existing and applicable industry standards in energy industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

I. Common Injuries & Damages

91. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

Data Breaches Increase an Individual's Risk of Identity Theft

92. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information, precisely as they have done here. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

93. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

94. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

95. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.³⁰

³⁰ "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are

96. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

97. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

98. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver’s license numbers) of Plaintiffs and the other Class Members.

99. Thus, even if certain information (such as driver’s license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

100. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-) (last visited on May 26, 2023).

Loss Of Time to Mitigate The Risk Of Identity Theft And Fraud

101. As a result of the recognized risk of identity theft, when a Data Breach occurs and an individual is notified by a company that their PII was compromised, as here, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

102. Thus, due to the actual and imminent risk of identity theft, the Notice Letter encourages Plaintiffs and Class Members to do the following:

We encourage you to enroll in the credit monitoring and identity protection services we are making available to you. Information about how to enroll in these services along with additional resources available to you are included in the *attached Steps You Can Take To Protect Your Information.*³¹

103. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer networks; contacting financial institutions to sort out fraudulent applications placed in their names; and monitoring credit reports and accounts for unauthorized activity, which may take years to discover and detect.

104. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."³²

³¹ Notice Letter.

³² See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

105. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.³³

106. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."³⁴

Diminution Of Value Of PII

107. PII is a valuable property right.³⁵ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

108. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other entities in custody of healthcare and medical information often purchase PII on the black market for the purpose of target marketing their products and services to the data breach

³³ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited July 7, 2022).

³⁴ See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Sep. 13, 2022) ("GAO Report").

³⁵ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

victims themselves. Insurance companies purchase and use wrongfully disclosed PII to adjust their insureds' medical insurance premiums.

109. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.³⁶

110. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.³⁷ In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{38,39} Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁴⁰

111. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

112. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable

³⁶ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Sep. 13, 2022).

³⁷ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

³⁸ <https://datacoup.com/>

³⁹ <https://digi.me/what-is-digime/>

⁴⁰ Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html>

consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

113. The fraudulent activity resulting from the Data Breach may not come to light for years.

114. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

115. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Credit And Identity Theft Monitoring is Reasonable & Necessary

116. Given the type of targeted attack in this case and sophisticated criminal activity, and the type of PII involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

117. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

118. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.⁴¹

119. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain

120. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay for energy products and/or services at Defendant, Plaintiffs and other reasonable consumers understood and expected that they were, in part, accepting and paying for the products and/or services and necessary data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received energy products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

J. Plaintiffs Experiences

Plaintiff Jessica Flagella

121. Plaintiff Jessica Flagella is a received services from Dollar Energy, who required that she provide it with substantial amounts of her and her minor children's PII.

⁴¹ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

122. At the time of the Data Breach—January 31, 2023 through February 5, 2023—Dollar Energy retained Plaintiff's PII in its system.

123. Plaintiff Flagella is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Flagella would not have provided her PII to Defendant had she known that Defendant would not reasonably safeguard it from unauthorized access.

124. Plaintiff Flagella first learned of the Data Breach after receiving a data breach notification letter from Dollar Energy, dated September 28, 2023, notifying her that Defendant suffered a data breach more than six months earlier and that her PII and her minor children's PII had been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendant.

125. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff has spent several hours dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

126. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available

for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

127. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

128. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

129. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

130. Plaintiff Flagella has a continuing interest in ensuring that her PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Cindy Tignor

131. Plaintiff Cindy Tignor is a former customer at Dollar Energy who obtained energy products and/or services from Defendant in or about 2021.

132. At the time of the Data Breach—January 31, 2023 through February 5, 2023—Dollar Energy retained Plaintiff's PII in its system.

133. Plaintiff Tignor is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Tignor would not have provided her PII to Defendant had she known that Defendant would not reasonably safeguard it from unauthorized access.

134. Plaintiff Tignor first learned of the Data Breach after receiving a data breach notification letter from Dollar Energy, dated September 28, 2023, notifying her that Defendant suffered a data breach more than six months earlier and that her PII had been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendant, including her name and Social Security number.

135. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: contacting changing passwords and resecuring her own computer network; contacting financial institutions to sort out fraudulent applications placed in her names; and monitoring credit reports and accounts for unauthorized activity, which may take years to discover and detect. Plaintiff has spent several hours dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

136. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

137. Plaintiff further suffered actual injury in the form of an identity thief using her PII to submit a fraudulent credit card application to Capital One, in or about March 2023, which, upon information and belief, was caused by the Data Breach.

138. Plaintiff further suffered actual injury in the form of an identity thief using her PII to submit a fraudulent credit card application to CBNA Bank, in or about October 2023, which, upon information and belief, was caused by the Data Breach.

139. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

140. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

141. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

142. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

143. Plaintiff Tignor has a continuing interest in ensuring that her PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

144. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated, pursuant to the Federal Rule of civil Procedure 23, for the following class defined as:

Nationwide Class

All individuals residing in the United States whose PII was compromised in the data breach first announced by Defendant in or about September 2023 (the “Class”).

145. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

146. Plaintiffs reserve the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

147. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Upon information and belief, at least 28,000 individuals were notified by Defendant of the Data Breach, according to the report submitted to the Maine Attorney’s General office.⁴² Moreover, the Class is apparently identifiable within Defendant’s records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

148. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

⁴² See <https://apps.web.mainecode.gov/online/aewebviewer/ME/40/862d1222-4fd2-482b-9651-c3eea92cc6c0.shtml> (last accessed Oct. 30, 2023).

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;
- b. Whether Defendant had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;
- c. Whether Defendant had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;
- k. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and,

1. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

138. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

139. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

140. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiffs has retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intends to prosecute this action vigorously.

141. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and

expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

142. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

143. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

144. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

145. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper

notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

146. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

147. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;
- e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and,
- f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members.

COUNT I
Negligence
(On behalf of Plaintiffs and All Class Members)

148. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above, as though fully stated herein.

149. Defendant required Plaintiffs and Class Members to submit non-public PII as a condition of obtaining energy products and/or services at Defendant.

150. Plaintiffs and the Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information and delete it once the employment relationship terminated.

151. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

152. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

153. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

154. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' PII; and,
- e. Failing to detect in a timely manner that Class Members' PII had been compromised.

155. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

156. Plaintiffs and the Class are within the class of persons that the FTC Act intended to protect.

157. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act intended to guard against.

158. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

159. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

160. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

161. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the energy industry.

162. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

163. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

164. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

165. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

166. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

167. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See Restatement (Second) of Torts § 302B.* Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

168. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

169. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

170. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

171. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Tignor experiencing fraud in the form of an identity thief using her PII to submit a credit card application to Capital One in or about March 2023; (ix) Plaintiff Tignor experiencing fraud in the

form of an identity thief using her PII to submit a credit card application to CBNA Bank in or about October 2023¹ and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

172. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

173. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

174. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

175. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

176. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and All Class Members)

177. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above, as though fully stated herein.

178. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant’s duty.

179. Defendant violated Section 5 of the FTC Act and similar state statutes by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant’s conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant’s systems.

180. Defendant’s violation of Section 5 of the FTC Act and similar state statutes constitutes negligence *per se*.

181. Class members are consumers within the class of persons Section 5 of the FTC Act and similar state statutes were intended to protect.

182. Moreover, the harm that has occurred is the type of harm the FTC Act and similar state statutes were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

183. As a direct and proximate result of Defendant’s conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy;

(ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Tignor experiencing fraud in the form of an identity thief using her PII to submit a credit card application to Capital One in or about March 2023; (ix) Plaintiff Tignor experiencing fraud in the form of an identity thief using her PII to submit a credit card application to CBNA Bank in or about October 2023; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

184. Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

185. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above, as though fully stated herein.

186. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of obtaining energy products and/or services at Defendant.

187. Plaintiffs and Class Members provided their PII to Defendant and made payments to or on their behalf to Defendant in exchange for (among other things) Defendant's promise to protect their PII from unauthorized disclosure and to delete it once it was no longer necessary to

maintain the PII for business purposes. Defendant additionally promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

188. On information and belief, Defendant further promised to and represented it would comply with industry standards and to make sure that Plaintiffs' and Class Members' PII would remain protected.

189. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

190. When Plaintiffs and Class Members provided their PII to Defendant as a condition obtaining energy products and/or services at Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

191. Defendant required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

192. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

193. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

194. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

195. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

196. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

197. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

198. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

199. Plaintiffs and Class Members are also entitled to nominal damages for the breach of implied contract.

200. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to The Class.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and All Class Members)

201. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above, as though fully stated herein.

202. This count is pleaded in the alternative to the breach of contract count above.

203. Plaintiffs and Class Members conferred a monetary benefit on Defendant by providing Defendant with payments for energy products and/or services as well as by providing their PII, and Defendant.

204. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

205. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof.

206. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

207. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

208. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

209. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

210. Plaintiffs and Class Members have no adequate remedy at law.

211. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff Tignor experiencing fraud in the form of an identity thief using her PII to submit a credit card application to Capital One in or about March 2023; (ix) Plaintiff Tignor experiencing fraud in the form of an identity thief using her PII to submit a credit card application to CBNA Bank in or about October 2023; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

212. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

213. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays for judgment as follows:

- A. For an Order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such

information when weighed against the privacy interests of Plaintiffs and Class Members;

- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;
- v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and securing checks;

- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;
- xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third

parties, as well as the steps affected individuals must take to protect themselves; and,

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

- D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Jury trial is demanded by Plaintiffs and members of the putative Class on all issues so triable.

Date: January 30, 2024

Respectfully Submitted,

By: /s/ Randi Kassan
Randi Kassan
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, LLC
100 Garden City Plaza
Garden City, NY 11530
Telephone: (212) 594-5300
rkassan@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, LLC
5335 Wisconsin Avenue NW
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

*Attorney for Plaintiffs and
the Proposed Class*

**Pro Hac Vice* application forthcoming